BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of BACCHIAZ et al

Application No. 09/764,729

Examiner:

Filed: January 17, 2001

Group Art Unit:

For: BIOMETRIC KEY

CLAIM OF FOREIGN PRIORITY

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231 on 3/19/01

Mark D. Passler Reg. No. 40,764

Commissioner for Patents
Washington, D.C. 20231

Sir:

Priority under the International Convention for the Protection of Industrial Property and under 35 U.S.C. §119 is hereby claimed for the above-identified patent application, based upon Australian Application No. PQ 7541 filed May 16, 2000, and a certified copy of this application is submitted herewith which perfects the Claim of Foreign Priority.

Respectfully submitted,

Date: 3/19/01

J. Rodman Steele, Jr.
Registration No. 25,931
Mark D. Passler
Registration No. 40,764
Akerman, Senterfitt & Eidson, P.A.
Esperante Building, Suite 400
222 Lakeview Avenue
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000

Docket No. 9300-1

P1009147;1

AUSTRALIA

Patent Office
Canberra

I, CASSANDRA RICHARDS, ACTING TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PQ 7541 for a patent by MONDAMI PTY LTD filed on 16 May 2000.

I further certify that pursuant to the provisions of Section 38(1) of the Patents Act 1990 a complete specification was filed on 16 November 2000 and it is an associated application to Provisional Application No. PQ 7541 and has been allocated No. 71644/00.

WITNESS my hand this
First day of February 2001

6

CASSANDRA RICHARDS
ACTING TEAM LEADER
EXAMINATION SUPPORT AND SALES

P/00/009
Regulation 3.2

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

Invention Title: "BIOMETRIC KEY"

The invention is described in the following statement:

"BIOMETRIC KEY"

This invention relates to a biometric key and more particularly relates to a biometric key having a key body which contains a biometric reader or sensor capable of capturing a key holder's biometric data and transmitting the data through the biometric reader or sensor to an external processor in order to validate authorised use of the key through biometric verification.

Currently keys are used for a wide variety of applications that comprise a mechanical or electromechanical cipher which carries coded information. One example of the latter is keys described in European Patent 472495 which has a specific mechanism located on opposed edges of the key which co-operates with a corresponding mechanism built into a mating lock cylinder before a locking system incorporating the lock cylinder may be opened.

Which such keys are simple to use, it will be appreciated that the level of security is not high because there is no means currently available for verifying that the person using the key is an authorised user. This means that while a conventional mechanical or electromechanical lock operated by a key presents physical access to a building such a key may be readily copied or it may be lost or given to other persons who may then gain access to the building on an unauthorised basis. Thus physical access to the building is provided by those in control of the key.

Conventional biometric control systems are well known and refer to encoding of a person's specific biometric features into a memory of the biometric control apparatus with an external process (e.g. storage memory, matching algorithm and return signal). A coded version of an authorised biometric feature can be stored. When verification is required, it is necessary for the user to present his biometric characteristic feature to the biometric control apparatus which then compares the biometric characteristic feature with the authorised biometric feature. If a match occurs, then the biometric control system permits access to a facility controlled by the biometric control system.

Biometrically secured control systems for preventing unauthorised use of vehicles are described in US Patent 5867802. This reference describes a method and system for restricting use of a vehicle to person(s) whose fingerprints match biometric data stored within a memory in the control system of the vehicle. A user's digitised fingerprints are stored in a ROM in the BIOS of a microcontroller or in a ROM accessed by a microcontroller. The microprocessor's primary task is that of executing instructions which are related to the operation of the vehicle such as regulation of the fuel flow rate and other tasks. Before the microprocessor can execute its instructions related to the primary task, it must complete and exit a conditional loop of instructions that relate to validating the

user's "real input" biometric data. Real scanned fingerprints must be compared with fingerprints(s) stored in ROM. If the result of the comparison is a match, then the operating loop is satisfied and the microprocessor can execute its instructions relating to operation of the vehicle. In US Patent 5607802 use is made of a conventional fingerprint scanning device and related circuitry coupled to the microprocessor. A key operated ignition switch is coupled to the microprocessor to provide a signal for providing power to the microprocessor before it may control operations related to the vehicle.

Another example of biometrically secured control systems is described in US Patent 5915936 which refers to a firearm which incorporates a pressure sensor for sensing grasping of a butt section of the firearm by a palm of the user as well as a scanning sensor for scanning a palm print of the user and generating a data signal representative of the scanned palm print after actuation of the pressure sensor. The firearm can only be used by authorised users wherein a memory unit stores data signals representative of the authorised users.

US Patent 5987155 refers to a biometric information input device having an integral smart card reader. The device provides co-operative operation of the smart card and the input device to provide user specific processing of biometric information provided by the user. Examples of biometric input devices referred to

in this reference are those incorporating a microphone or those which comprise a contact imaging device such as a fingerprint scanner.

The abovementioned prior art references are illustrative of biometric control systems which can only be operated upon use of a vehicle ignition key as described in US Patent 5867802, a pressure sensor in the case of US Patent 5915936 or a smart card in the case of US Patent 5987155. It therefore will be appreciated that such conventional biometric control systems are non versatile in being restricted to a specific application, and also require the use of additional structure relative to the specific application. Thus for example the biometric input device of US 5987155 requires as an essential component a card slot for acceptance of the smart card.

It is an object of the present invention to provide a biometric key which may reduce the disadvantages of the prior art discussed above.

The biometric key of the invention has a key body incorporating a biometric sensor. Preferably the key body has contact means which contacts mating contact means in a reader to send an electrical signal.

The key body may be similar to a conventional key which unlock mechanical locks wherein the key has a blade with a plurality of wards that co-operate with lock tumblers in a conventional manner to unlock the mechanical lock as hereinafter described. The

key body may also have a handle or gripping part which may have the biometric sensor applied or attached thereto or embedded therein. Preferably the sensor is accommodated within a mating recess of the key body and is provided with contacts or pins forming one example of the contact means which may engage with a circuit board also accommodated within the lock body. Preferably the sensor is surrounded by an insulator insert.

Alternatively the key body may omit wards and have a blade or end portion which engages with a mating slot in a stationary reader as described hereinafter. In this embodiment the reader may interface with a peripheral processor, whereby upon recognition of an authorised signal by the reader, an unlocking action may be effected.

The sensor may be a solid state sensor manufactured by Pollex and the sensor may scan an appropriate biometric characteristic of the key holder. Alternatively the sensor may be manufactured by Thompson, Veridicon or Harris which are all well known solid state manufacturers. The scanning sensor may be carried out using a number of techniques which may include capacitance, resistance, thermal imagery, structure geometry, bone structure or vein structure. Suitably the scanning sensor scans a fingerprint or thumb print.

The key body may also have embedded therein a smart card chip such as a wired logic chip also known as an "intelligent

memory" chip which has inbuilt logic. Embedded processor chips, added to the key body, may contain memory and local processor capabilities. The embedded processor chip, embedded within the key body, may be used to encrypt/decrypt data, which makes this type of biometric key a unique person identification key. The biometric key data processing permits also the dynamic storage management, which enables realisation of flexible multifunctional features.

Examples of use of the biometric key of the invention may be as an ignition key of a vehicle, a key to a storage facility such as a drawer, lid of a box, security door, security window, to operate an elevator or lift or to initiate actuation of an electric motor, hydraulic motor, engine or other form of drive means or even hydraulic or pneumatically actuated ram assemblies.

It therefore will be appreciated from the foregoing that the biometric key of the invention is extremely versatile having many applications or uses and also extremely simple in structure to at least partially overcome the disadvantages of conventional biometric control systems as described above. The biometric key of the invention also involves a high degree of security to overcome the problems of conventional keys as described above.

Reference may now be made to a preferred embodiment of the present invention as described in the accompanying drawings wherein:

FIG. 1 is a view of the biometric key of the invention held in a person's hand;

FIG. 2 is a perspective view of a biometric key of the invention which is inserted into a corresponding lock cylinder of a lock body;

FIG. 3 is an exploded perspective view of the key of FIG. 1 showing all parts thereof;

FIG. 4 is an exploded perspective view of a barrel of the lock cylinder of FIG. 2 separated from the lock cylinder of FIG. 1;

FIG. 5 is a plan view of the biometric key of the invention shown in FIG. 1 inserted in the barrel;

FIG. 6 is a section through line A-A of FIG. 5;

FIG. 6A is an exploded view of the components of FIG. 6;

FIG. 7 is a section through line B-B of FIG. 5;

FIG. 8 is a detailed view of contact detail shown in FIG. 7;

FIG. 8A is an exploded view of the components of FIG. 8;

FIG. 9 is a section through line C-C of FIG. 4;

FIG. 10 is a detailed view of contact detail shown in FIG. 8;

FIG. 10A is an exploded view of the components of FIG.

10;

FIG. 11 is a plan view of a biometric key of the invention inserted in a barrel of different shape to that shown in FIG. 4;

FIG. 12 is a section through line A-A of FIG. 11;

FIG. 13 is a section through line D-D of FIG. 11;

FIG. 14 is a detailed view of a contact shown in FIG. 13;

FIG. 15 is an exploded perspective view of the key of FIG. 11 separated from the barrel;

FIG. 16 is a perspective view of the barrel of FIG. 15 from another orientation;

FIG. 17 is a detailed view of a contact shown in FIG. 15;

FIG. 18 is a block diagram describing the chain of events upon operation of the biometric key of the invention; and

FIG. 19 is a schematic view showing enrollment of biometric data signature via an external host computer.

In FIG. 1 there is provided a biometric key 10 of the invention held in the hand 11 having control portals 12. The key 10 has a key body 13 and a sensor 14 being contacted by thumb 15. The key 10 is also provided with blade 16 having wards 17.

In FIG. 2 the key 10 is shown inserted into lock cylinder 18 which is fitted into mating aperture 19 of lock body 20 having lock tongue 21. The cylinder 18 has contact portals 22 and also has upper component 23 which fits into mating recess 24. The cylinder

18 is also provided with wires 25. The lock body 20 is of mechanical nature having a custom wire bus (not shown).

In FIG. 3 the key 10 is shown having components in the form of the sensor 14, insulator insert 27 and circuit board 28 which fits into recess 29 of insulator insert 27. Insulator insert 27 is slidably attached to key body 13 and bonded thereto. The circuit board 28 is shown on both sides as is key body 13 which is formed from sensor 14, insulator insert 27 and circuit board 28 as illustrated. Sensor 14 fits within recess 30 of insulator 27. The circuit board 28 has wire leads 28A which bond to corresponding tabs 26 on sensor 14.

In FIG. 4 the key 10 is shown fitted into a mating barrel 31 having contact portals 32. The barrel 31 has flange 33 and end 34 having a slot 35. The barrel 31 also has tumblers 36.

Contact portals 32 touch mating contact portals 22. The contact portals 22 exchange electronic signals with an external processor as hereinafter described through lock body 20. The electronic interface with the outside processor may comprise USB, parallel, serial or IEEE1384 firewire signals. The outside processor may also provide return electrical signals that control a linear motor or solenoid 38 which releases a cylindrical locking pin 39 which fits within bore 40 or cylinder 18. Motor 38 has a spring loaded piston 41 which engages with aperture 42 of locking pin 39. Motor 38 also

fits within mating socket 43 of cylinder 18. Locking pin 39 has projection 44 which engages with slot 35 of barrel 31. Motor 38 also has contacts 47 which engage with wires 25. There is also provided trigger latch 48 of cylinder 18 shown in the locked position and which is located on rotatable collar 49 of cylinder 18. The trigger latch 48 engages with slot 50 in the unlocked position. The lock 20 controls access in two different ways i.e. requiring a valid return signal from the remote or outside processor to unlock the locking pin 39 as well as tumblers 36. When unlocking of lock body 20 is initiated, piston 41 retracts within motor 38 and latch 48 engages with slot 50. The upper component 23 of cylinder 18 has screw threaded attachment holes 51A which facilitate attachment to lock body 20.

FIG. 5 shows key 10 inserted into barrel 31 and FIG. 6 is take along line A-A of FIG. 5. In FIG. 6 there is shown individual insulators 50A and 51 which contact pins 52 and 53. A closer detail is shown in FIG. 6A which shows insulators 50A and 51 engaging in a press fit within key body 13 and contact pins 52 and 53 engaging within a press fit within mating insulators 50A and 51. Contact pins 52 and 53 have barbed points 52A which drive into a solder puddle on circuit board 28.

FIG. 7 is taken along line B-B of FIG. 5. There is shown contact pin 55 which is a sliding fit within insulator body 54, and fuzz

button 57. The purpose of fuzz button 57 is to provide electrical continuity between contact pins 55 and 56 under the influence of pressure from spring 58. A closer detail of this arrangement is shown in FIG. 8. An exploded view is also shown in FIG. 8A.

FIG. 9 is a section along line C-C of FIG. 4 and shows insulator body 63 which is bonded within barrel 31, contact pin 62 adapted for press fit within insulator body 63, fuzz button 64 and additional contact pin 65 which has a sliding fit within insulator body 63. An exploded view is shown in FIG. 10A.

In the embodiment shown in FIGS. 1-9 the fingerprint pattern captured on sensor 14 is converted into a peripheral reader or processor such as that marketed under the trademark Pollex POLPass or to a reader or processor within lock body 20 e.g. within cylinder 18. Preferably both the extraction and matching programs are stored in the memory of the processor.

The peripheral process may be operated in either a stand alone environment (platform independent) or aided with a remote peripheral-computer connected by a variety of means including serial, parallel, or USB connection. The processor may comprise a Digital Signal Process (DSP) unit or ASIC processor. The processor captures and extracts a biocode of the fingerprint scanned by the biometric key. The biocode is a fingerprint map or digital signature that permits identity verification of a person. The extraction and matching

algorithm is based upon minutiae comparison. The maximum size of a biocode in this particular context may be 254 bytes. The processor in some cases can manage up to 2048 biocodes in its own database or a remote host computer may manage the database if more biocodes are needed. In order to take full advantage of the features available, such as administrative reports and user queries, a remote computer is suggested to interface to the processor board.

The processor may be a self-contained board using only an external power source, an interface to the sensor, and a serial connection to the host processor. The processor may also contain on-board RAM, ROM, communications interface, fingerprint recognition software and database manager, all integrated into an optimised device. It is the task of the system integrator to fulfill the relevant specification for the entire system operation.

There is a variety of enrollment means to enter a biocode into the processor database. The most common is a remote host computer via a serial connection. A Smartcard Reader may also be used in conjunction with a 10-key pad to control the processor. There is a multitude of ways to initiate administrator functions in a stand alone environment.

The processor may also enroll biocodes directly to the point of origin via the key. Users are grouped into two categories: administrator and regular users. The administrator registers, checks

and deletes the authorised people into the database. Template registration of a new user takes less than a second. After the biocode is registered, access is granted within a split second after positioning the finger on the sensor.

In FIG. 11 there is shown another alternative embodiment of the invention wherein key 10A is fitted within a stationary or static reader 18A and electrical continuity is provided by FIGS. 12 and 13, which represent sections along lines A-A and D-D of FIG. 11 and which relevant contact detail is shown in a similar manner as shown in FIGS. 6 and FIG. 8. In FIGS. 12 and 13 key 10A having key body 13A and contact portals 12 makes contact with contact pins 52 and 53 which are bounded by insulators 50A and 51 as described previously. Contact pins 52 and 53 touch mating contacts 56 which touch spring 58 and wiring 66. Wiring 66 is attached to fuzz button 57 by solder 67 as shown in FIG. 14. Key 10A is inserted in aperture 68 of reader 18A as shown in FIGS. 16-17. Wiring 66 is bonded to wire access grooves 69 which are shown in FIGS. 13 and 17. Reader 18A is also provided with a light emitting diode 70 which is a visual signal for acceptance (i.e. green) or rejection of the signal (i.e. red). Wiring 66 has contactors 66A, 66B, 66C and 67D as shown in FIG. 17.

Reader 18A may be mounted inside a drawer, box, housing of any security system whereby reader 18A may be wired to

an encoder (not shown) in the security system which requires access by biometric key 10A. Thus in this embodiment there is no requirement of a mechanical or electromechanical lock body 20 as shown in the embodiment of FIGS. 1-10.

The key 10A may also include a smart card chip 14A shown on the same side as sensor 14 or on the opposite or obverse side which is described in greater detail hereinafter.

An encoder will house appropriate software to analyse and share any number of authorised biometric signals.

In another aspect of the invention there is also provided a reader having contact means which contacts or touches the contact means of key 10 or 10A i.e. in one example contact portals 12 of key 10A will touch contacts 66A, 66B, 66C and 66D as shown in FIG. 15 or contact portals 12 of key 10 will contact portals 22 of cylinder 18 via intermediate portals 36 of barrel 31.

Thus the invention may include within its scope the abovementioned reader in the form of reader 18 or reader 18A. The invention may also include the barrel 31 per se.

The smart card chip 14A may comprise an integrated circuit with ISO 7816 interface and/or a processor integrated circuit and/or a personal identity token containing IC-S.

4

In FIG. 18 there is shown a block diagram representing

the chain of events upon use of the biometric key of the invention wherein the following events take place, i.e.

(i) the key 10 or 10A is inserted into the reader within cylinder 18 or reader 18A;

(ii) the key contacts make connection with the reader contacts;

(iii) power is provided to the sensor 14 in the key 10 or 10A, via the reader, from an external source;

(iv) biometric is read through the sensor 14, and data is passed to the reader through the key contacts and sent to the processor;

(v) the processor extracts biometric data signature, and compares to previously stored biometric data signature for match;

(vi) if a match exists, the external signal is latched (i.e. open/closed); and

(vii) the key 10 or 10A is removed from the reader.

In FIG. 19 there is shown a schematic diagram how enrollment of biometric data signature may be accomplished via an external host computer whereby:

(a) the external host computer software requests personal and/or demographic information relative to the authorised user;

(b) the biometric data signature is captured from the sensor through the key, via the reader interfaced to external host computer;

(c) personal and/or demographic information is stored with biometric data signature and stored within database;

(d) a search is performed against the database for previous enrollments (i.e. prevents multiple enrollments under assumed names);

(e) if not found, authorised user is enrolled into database;

(f) if found, enrollment is denied; and

(g) database located on processor board is updated to reflect new enrollment.

It will be appreciated from the foregoing that the biometric key of the invention is versatile in operation, has relatively simple structure and provides a high degree of security.

Dated this Sixteenth Day of May 2000

MONDAMI PTY LTD

by their Patent Attorneys

FISHER ADAMS KELLY

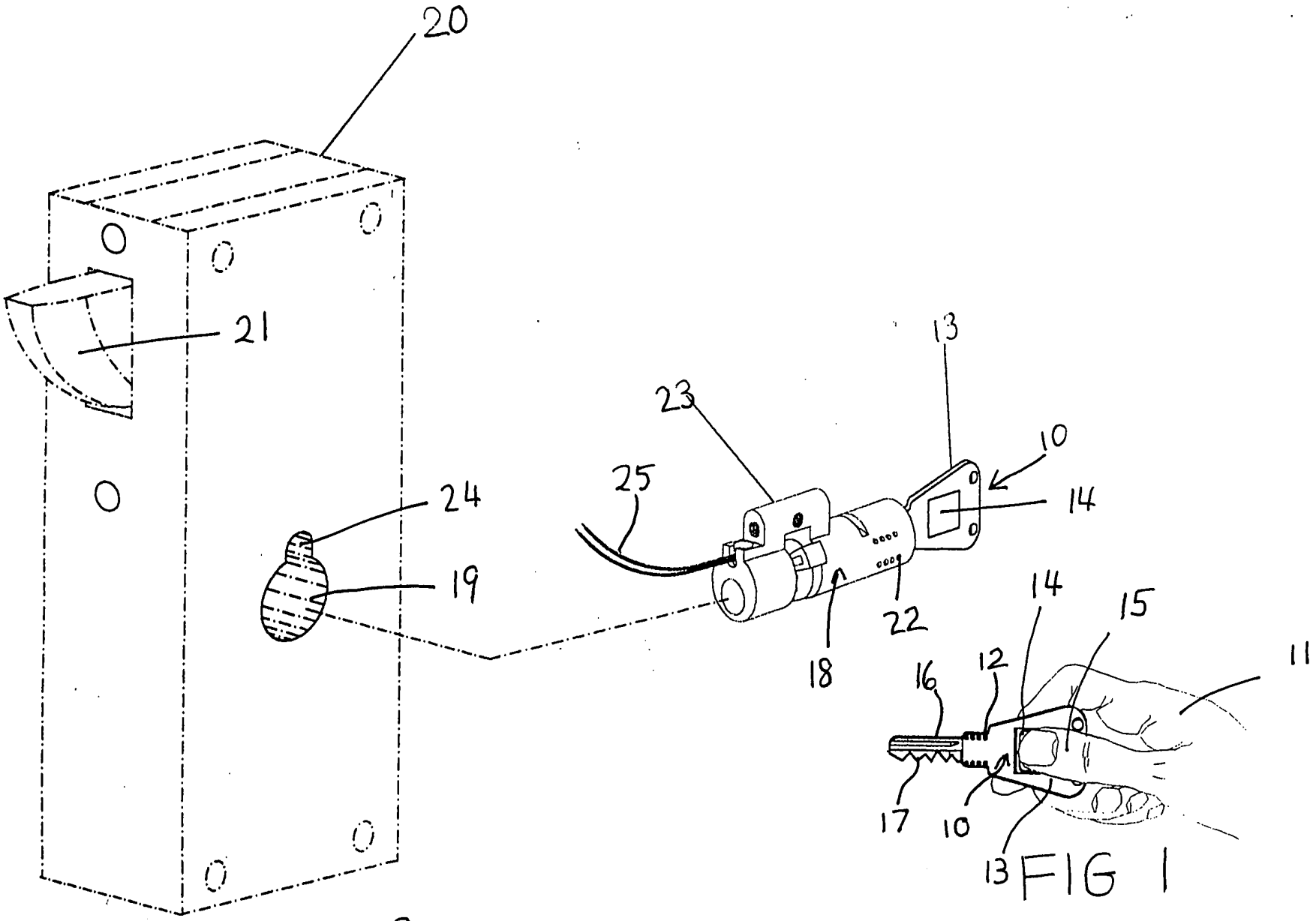


FIG 2

FIG 1

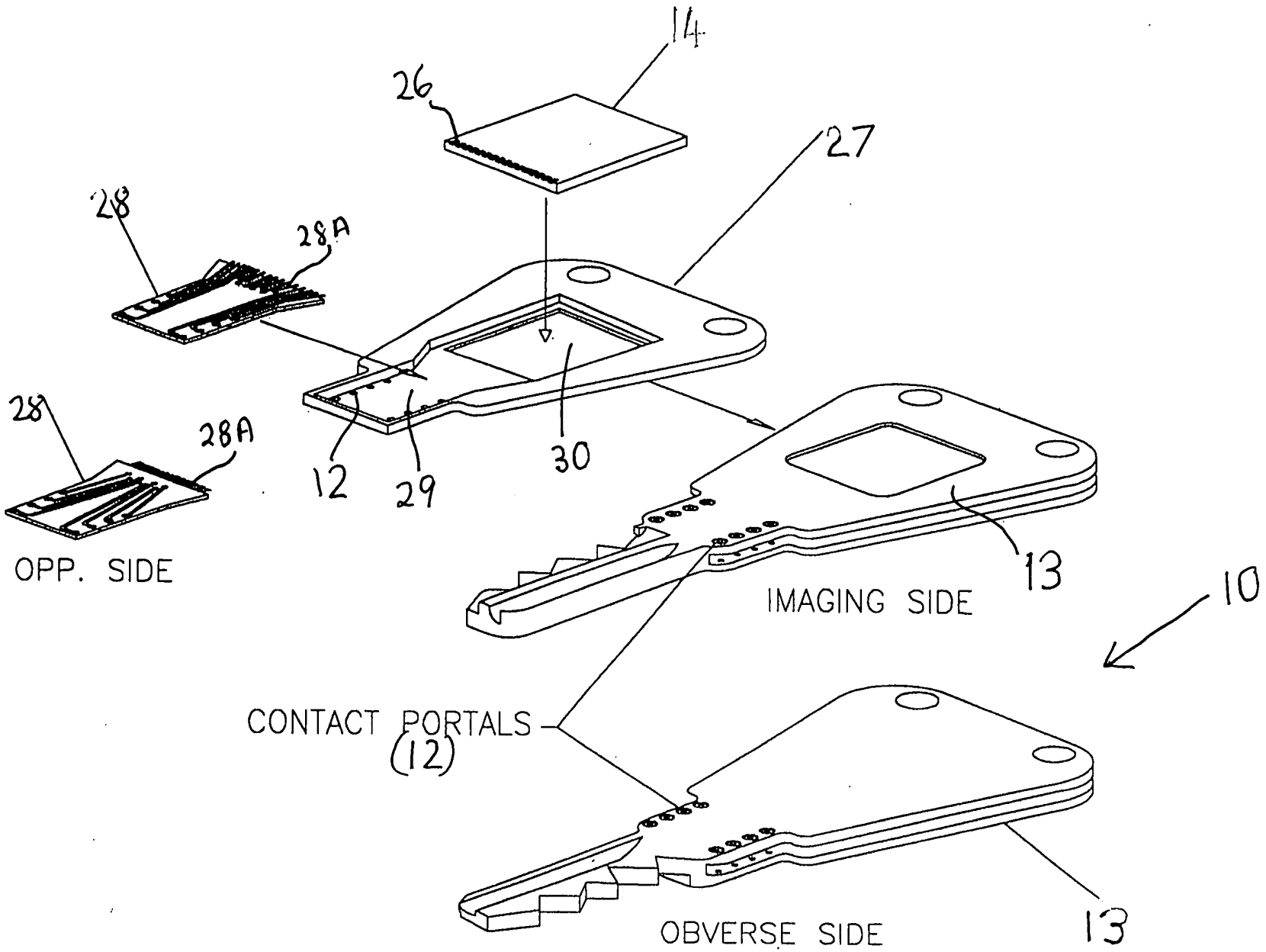

14
26
27
28
28A
28
28A
12
29
30
OPP. SIDE
IMAGING SIDE
13
10
CONTACT PORTALS
(12)
OBVERSE SIDE
13

FIG 3

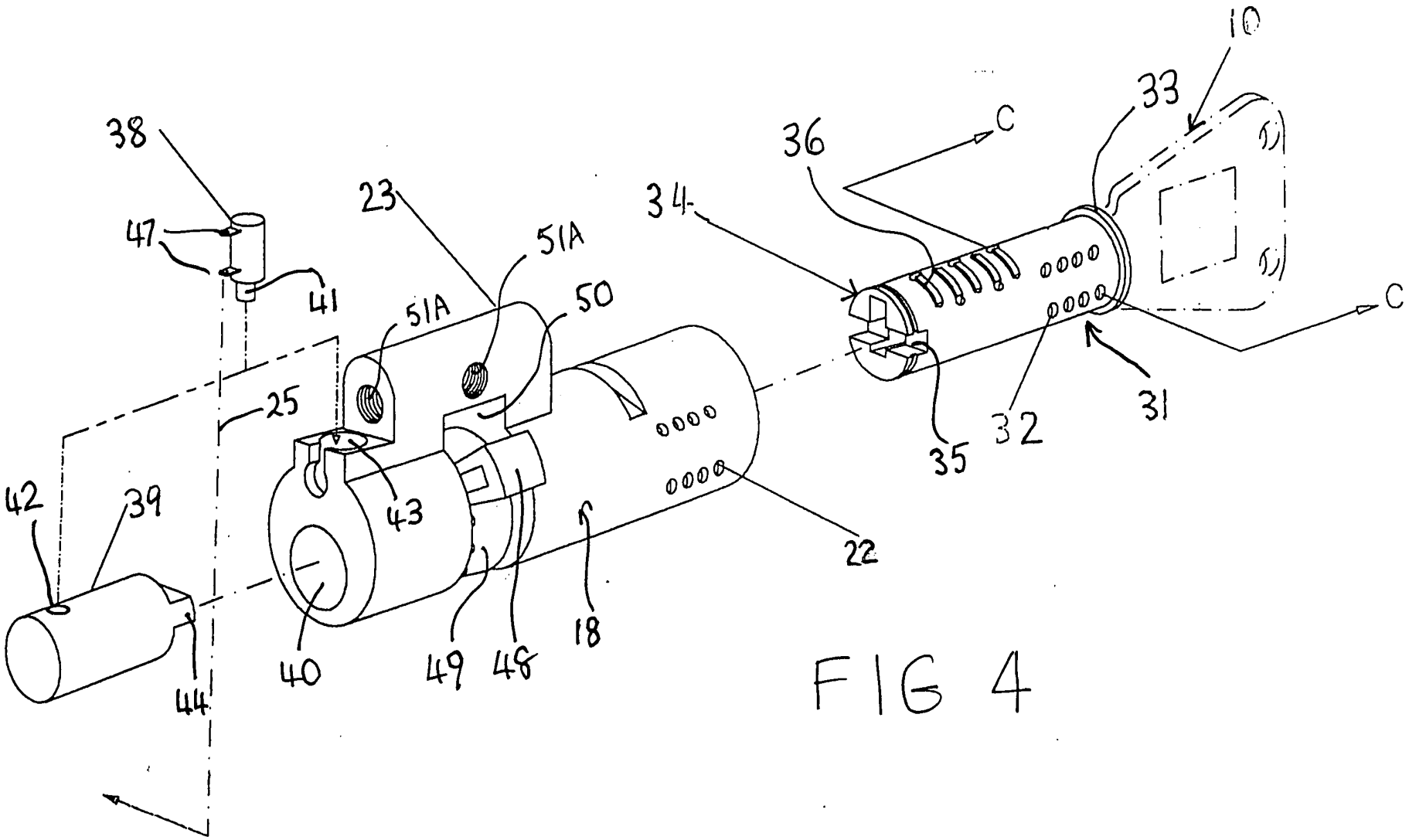
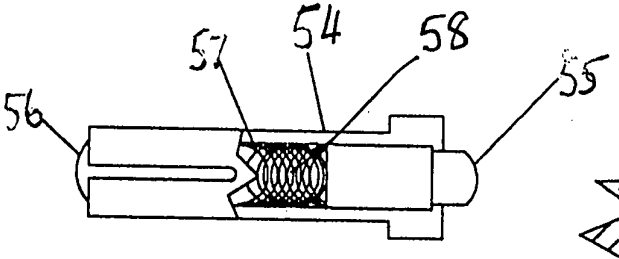
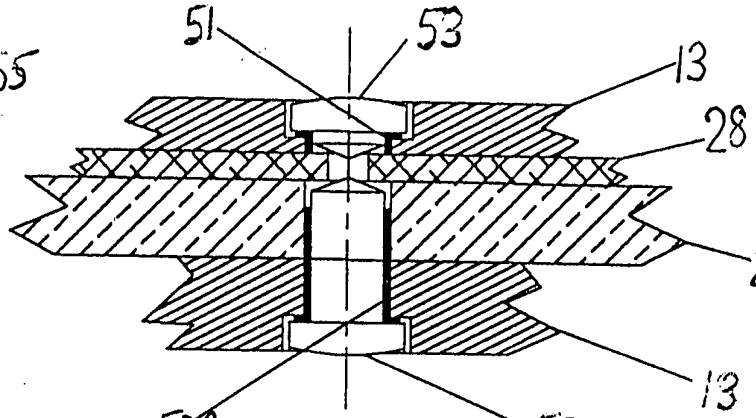

38
47
41
23
51A
51A
50
25
43
42
39
40
49
48
18
22
44
34
36
C
33
10
C
35
32
31

FIG 4



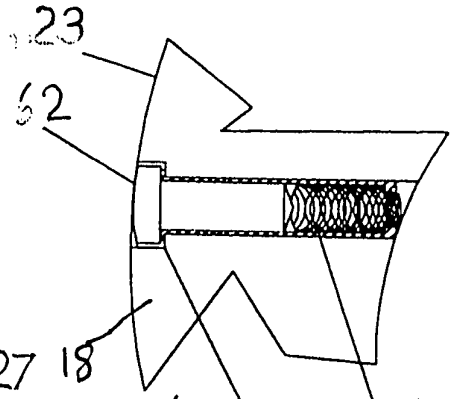
CONTACT DETAIL

FIG 8



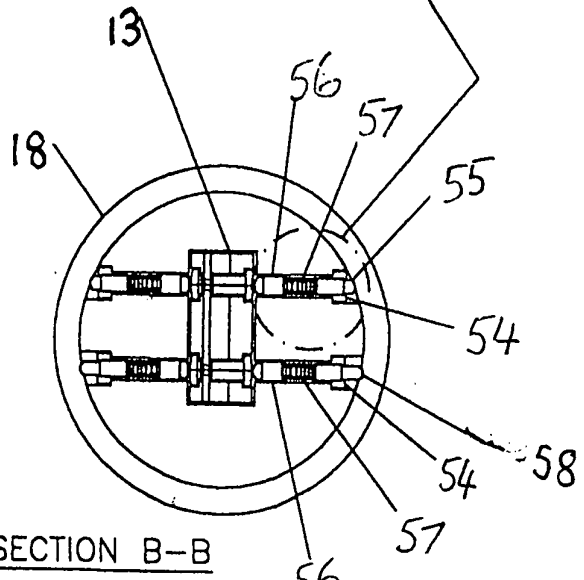
SECTION A–A

FIG 6



CONTACT DETAIL

FIG 10



SECTION B–B

FIG 7

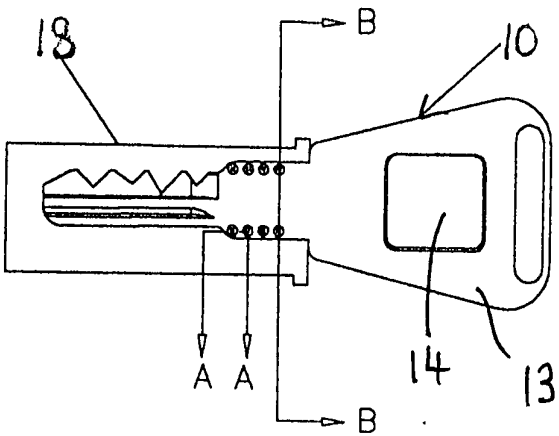
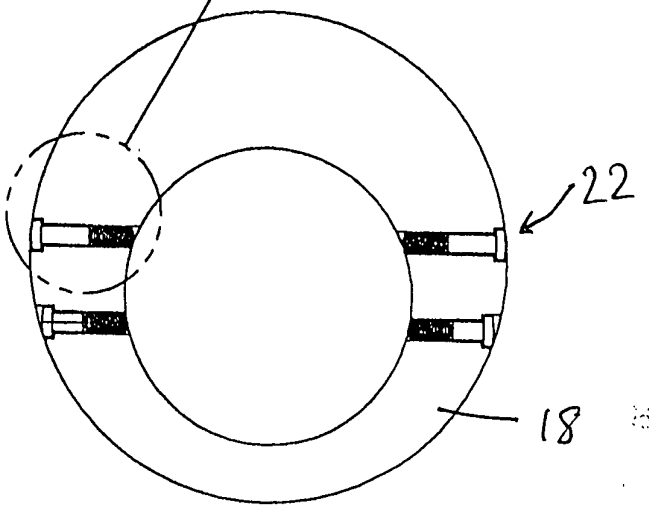


FIG 5



SECTION C–C

FIG 9

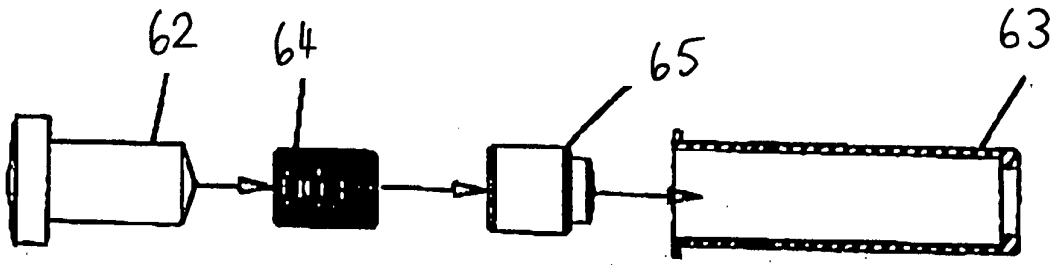


FIG 10A

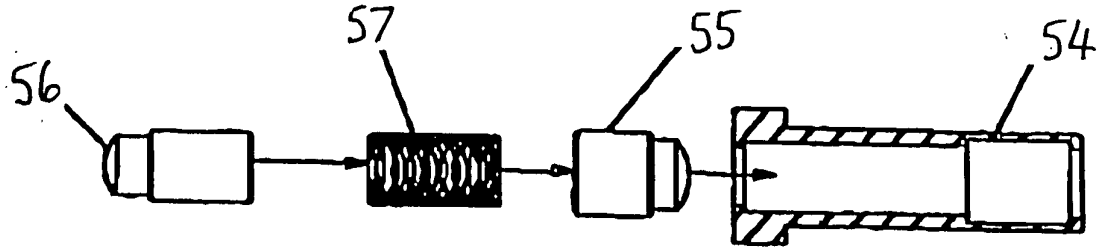


FIG 8A

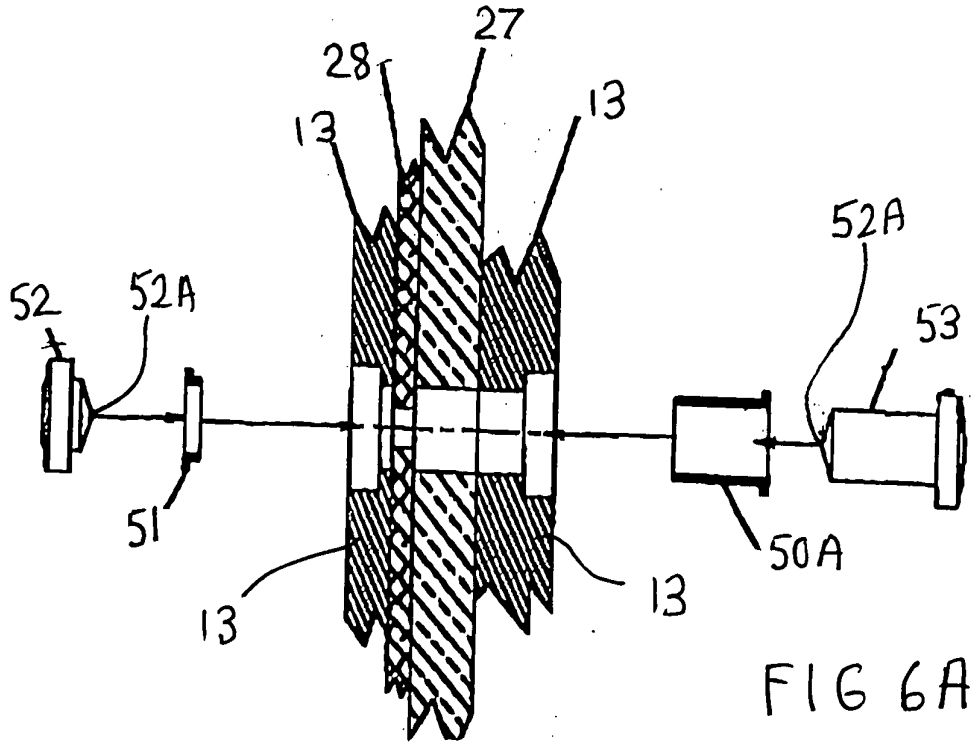


FIG 6A

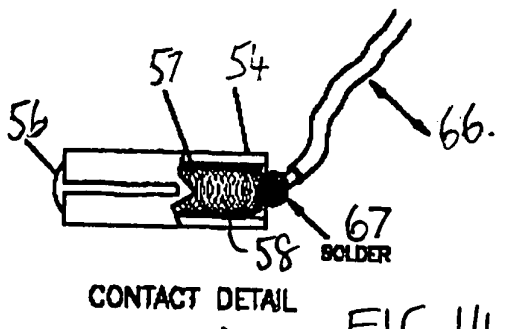


FIG 14

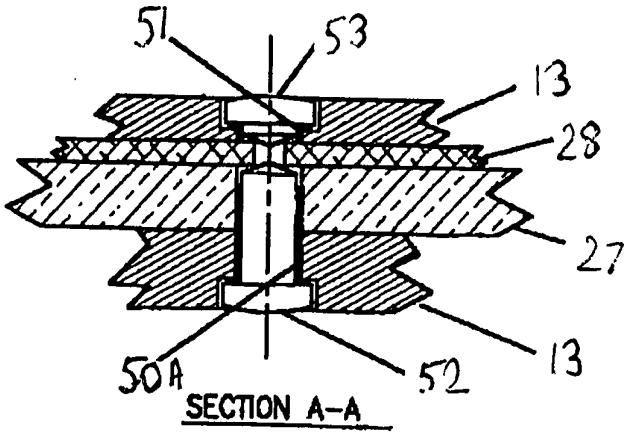


FIG 12

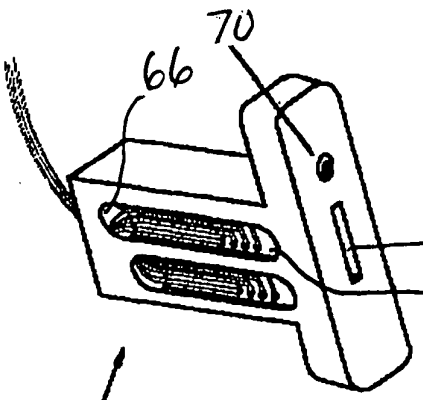


FIG 16

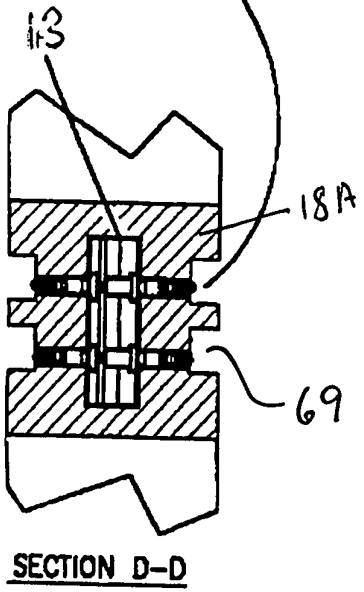


FIG 13

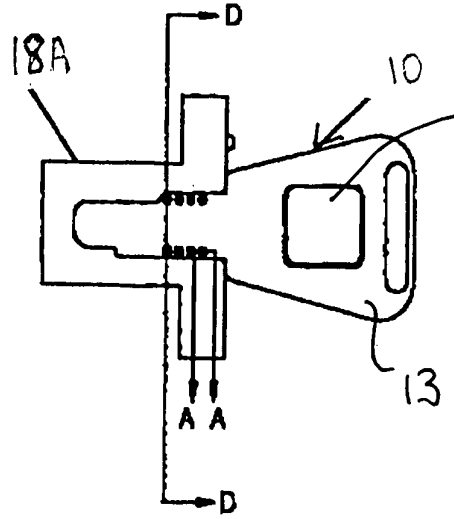


FIG 11

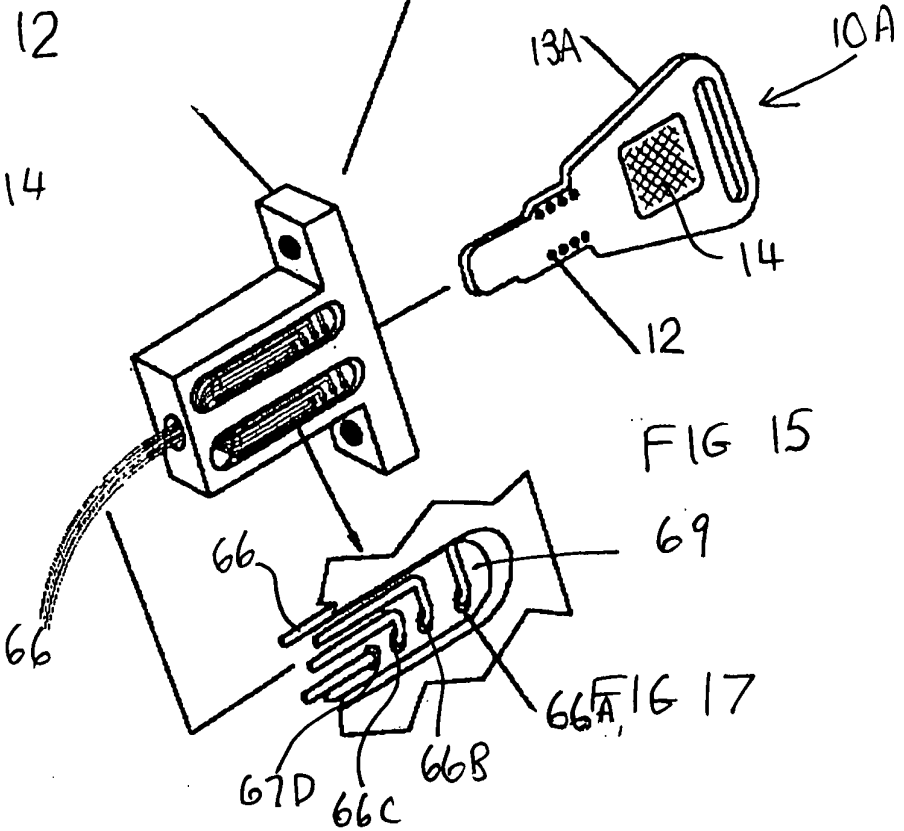


FIG 15

FIG 17

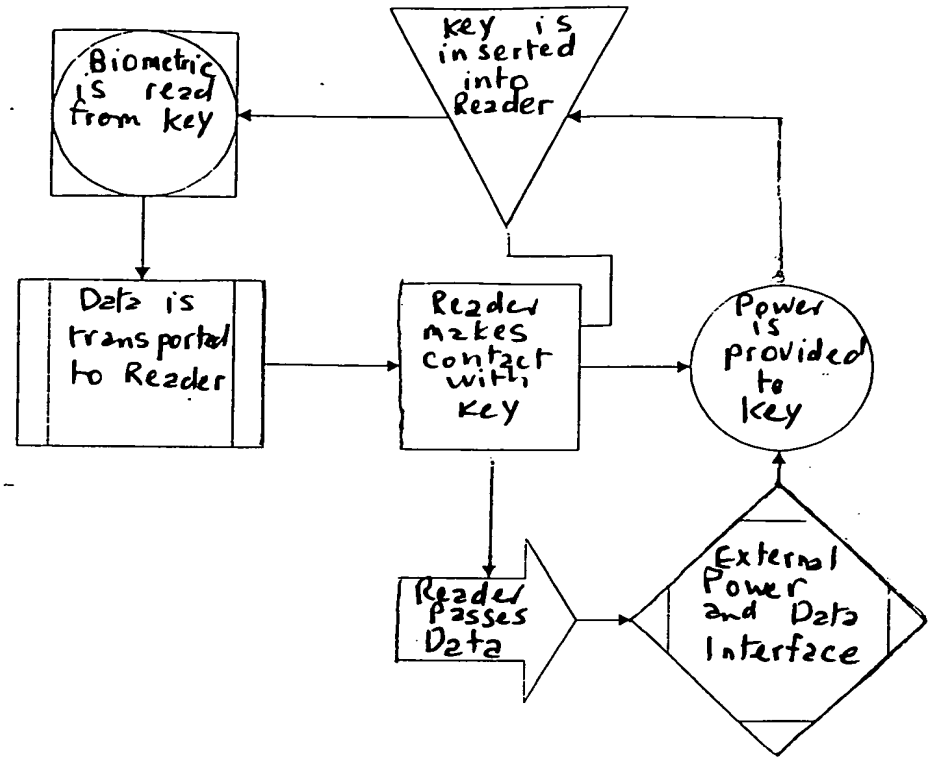

Biometric is read from key
key is inserted into Reader
Data is transported to Reader
Reader makes contact with key
Power is provided to key
Reader passes Data
External Power and Data Interface

FIG 18

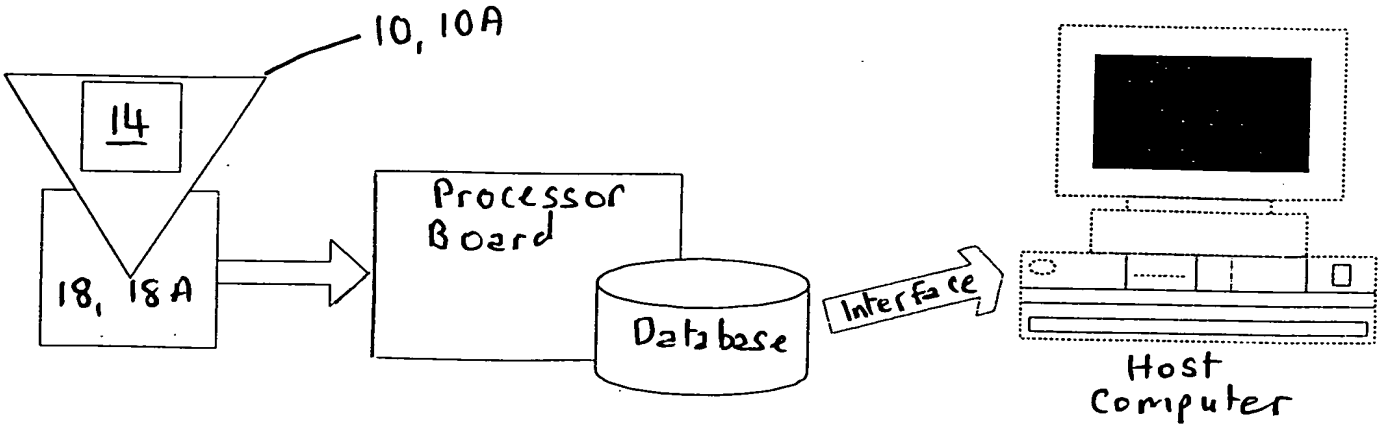

10, 10A
14
18, 18A
Processor Board
Database
Interface
Host Computer

FIG 19